



GTS Computer Service
PO Box 222
Haskell, NJ 07420
Phone 973 835-4738
E-mail service@gtscomputerservice.com
Web <http://www.gtscomputerservice.com>

Malware Information

Understanding, Preventing, and Removing Malware

Revised June 13, 2013

See also the Companion Document - “How to Use your Malware Tools.”

What is Malware?

Malware means malicious software. Although many use the term virus as a generic description of infections, there are many different kinds of malware. Technical types of malware include Viruses, Trojans, Rootkits, Spyware, Worms, malicious Active X controls, and malicious Browser Helper Objects.

Functionally malware types may be described as spyware, adware, browser hijackers, key loggers, scare ware, botnets, etc. The technical definitions can be complicated, and it's not necessary to know them. It is, though, important to be aware that malware has become ever more sophisticated and varied, and proper security practices and user caution are vital to prevention.

The impact of malware can range from a minor annoyance (e.g. pop up ads) to a serious security threat involving identity theft or financial fraud. It may work invisibly in the background or may take over your computer and demand payment in a false offer to release it and get your credit card information. Infections often cause poor computer performance and crashes.

Who Creates Malware?

In the early years of the personal computer, malware tended to be created as a form of pure vandalism or for a technical challenge. Today most malware is created and distributed by organized crime groups (often based in Eastern Europe, Russia, and China) with a profit motive. These groups employ sophisticated programmers, and share and resell technical how-to information in a black market.

How Do I Know If My Computer Is Infected?

Pop up ads, especially if your Internet browser is not open, are a strong indication. Firewall alerts that a program you don't recognize is trying to communicate may also indicate infection. A change in home page that will not allow resetting indicates a browser hijacker. Computer crashes, problems with programs, and generally poor performance *might* indicate Malware. Sometimes Malware will be present with no visible indication.

How is Malware Installed?

NOTE: As Windows (and especially Internet Explorer) has become more resistant to malware, hackers are increasingly targeting 3rd party software which users often fail to update as security fixes are released.

- “Drive by” infections may be acquired simply by viewing a Web page or Email message if your computer is not properly secured and up to date.
- Infected Adobe reader (PDF) documents, Flash videos, and Java applets may infect your computer especially if you're not keeping the respective programs up to date with the latest versions and security updates..
- Free programs (including games and hoax computer utilities), Email attachments, and downloads through instant messaging programs, social media sites, and file sharing services (like Torrent) are common sources of infection.
- Web sites offering items like shopping rebates and coupons, games, and pornography are common sources of Malware.
- Some browser tool bars contain Malware. Tool bars should only be installed from trusted Web sites (e.g. Google, Yahoo,).
- Pop up messages like “Your computer is not optimized or is infected” are almost always a hoax trying to trick you into downloading Malware.
- There are many infected files exchanged through Social Media sources like Facebook. Be very careful about downloading files from these sites.

- Once users suspect an infection, they often search for removal tools and make the problem worse by downloading or buying hoax programs which install additional infections.

How To Avoid Malware

It is difficult to completely protect against Malware. User vigilance is critical. The following items will greatly reduce the likelihood of infection.

- Keep your antivirus software up to date.
 - NOTE: No Antivirus program is 100% effective in preventing or removing Malware, but they will stop many common threats.
- Process Microsoft Important and Critical Windows Updates and Office Updates regularly.
 - This is extremely important because malware purveyors intensively target known Windows and Internet Explorer vulnerabilities which the updates address.
- Consider using an alternative web browser. Internet Explorer has had many security weaknesses over the years. Although newer versions of Internet Explorer are improved, using an alternative browser (e.g. Firefox or Chrome) may be helpful especially if you are running an older version of Windows (e.g. Windows XP) that cannot use the latest versions of Internet Explorer.
- Use a firewall. Starting with Windows XP Service Pack 2 the built-in Windows firewall is sufficient.
- Never accept unknown pop up prompts to do anything to your computer. Close pop up windows with the X in upper right. Especially, don't trust any Malware cleaner or computer maintenance tool advertised with pop ups or found in web searches. Many of them are hoax programs which actually install Malware..
- Don't open Email attachments unless you're certain they are legitimate.
- Don't accept Instant Messaging connections or file transfers from unknown sources.
- Be very cautious about downloading free programs and tool bars. Use only reliable sources.
- Peer Networks – There are many infected files distributed through peer network services like Torrent. If you do use such services, be very careful selecting any downloads.
- Use SpywareBlaster to provide additional protection and update its protections regularly. (See companion document.)
- Standard vs. Administrator User – It is best to use a Standard user account for day to day computer use rather than an Administrator account. This may help prevent infection and can limit the damage malware causes.

How To Remove Malware?

WARNING: Do Not search for and download unknown Anti-Malware programs or other “security or tune-up / optimization” programs! These are often hoaxes which will make the situation worse.

. There are some good free programs that can sometimes remove infections that antivirus programs cannot. GTS often installs several or all of these for you. **See the Companion Document “How to Use your Malware Tools.” which explains how to use these programs.**

Although the programs discussed in the companion document remove many common infections, they are not always effective. Severe infections often require professional help. The complexity of some current infection items requires specialized expertise and knowledge to remove. Less skilled technicians may not know how to remove severe infections and will often recommend wiping your hard drive. At GTS Computer Service we rarely find such extreme measures to be necessary. In the rare case where a system is too badly damaged to repair and must be reinstalled, we use scrupulous care to preserve your personal files.